REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
02-07-2008	Final Report	12-Aug-2003 - 31-Mar-2008

4. TITLE AND SUBTITLE
Quantum Search and Beyond

5a. CONTRACT NUMBER

5b. GRANT NUMBER
DAAD19-03-C-0096

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS
Lov K. Grover

5d. PROJECT NUMBER
611102
611102

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Lucent Technology
600 Mountain Avenue
PO Box 636
Murray Hill, NJ 07974 -0636

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
45005-PH-QC.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
Ten years ago, the quantum search algorithm was designed to provide a way of searching a space of N items in only □N steps. In the last ten years, it has been used as a building block for numerous applications, both physical and algorithmic - these are as diverse as precision measurement and communication complexity. It has been generalized to the amplitude amplification principle in which form it can be used to give a

15. SUBJECT TERMS
quantum searching - partial quantum searching, fixed-point quantum searching, Super-linear amplitude amplification, quantum search algorithms.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Lov Grover
U	U	U	SAR		19b. TELEPHONE NUMBER 908-582-2677

Report Title

Quantum Search and Beyond

ABSTRACT

Ten years ago, the quantum search algorithm was designed to provide a way of searching a space of N items in only □N steps. In the last ten years, it has been used as a building block for numerous applications, both physical and algorithmic - these are as diverse as precision measurement and communication complexity. It has been generalized to the amplitude amplification principle in which form it can be used to give a square-root speed-up to almost any probabilistic algorithm. Our research during this period has led to further developments into the applications of quantum searching, including three new variants of quantum searching - partial quantum searching, fixed point quantum searching & super-linear amplitude amplification.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Papers that appeared during this period

1. Quantum State Targeting Terry Rudolph and Rob Spekkens. quantph/0310060 Phys. Rev. A. 70, 052306 (2004).
2. How significant are the known collision and element distinctness quantum algorithms? Lov Grover and Terry Rudolph quant-ph/0309123 Journal Quantum Information & Computation ,4, 201 (2004).
3. Photon number superselection and the entangled coherent state representation Barry C. Sanders, Stephen D. Bartlett, Terry Rudolph, Peter L. Knight quant-ph/0306076 Phys. Rev. A. 68, 042329 (2003).
4. On the communication complexity of establishing a shared reference frame Terry Rudolph and Lov Grover quant-ph/0306017 Phys. Rev. Lett. 91, 217905 (2003). (The key idea in our paper on communication complexity of a shared reference frame was turned into an optical phase estimation style problem the experiment of which was published in Nature: http://arxiv.org/abs/0709.2996)
5. On continuous-variable entanglement with and without phase references, S.J. van Enk, Terry Rudolph quant-ph/0303096
6. Unambiguous discrimination of mixed states, Terry Rudolph, Robert W. Spekkens and Peter Shipley Turner quant-ph/0303071 Phys. Rev. A. 68, R010301 (2003).
7. Classical and quantum communication without a shared reference frame, Stephen D. Bartlett, Terry Rudolph, R. W. Spekkens, quant-ph/0302111 Phys. Rev. Lett. 89, 227901 (2001).
8. Quantum communication protocols using the vacuum, Xiatra Anderson, S.J. van Enk, Terry Rudolph, quant-ph/0302091 Journal Quantum Information & Computation, 3, 423 (2003).
9. A 2 rebit gate universal for quantum computing Terry Rudolph and Lov Grover quant-ph/0210187
10. Creating superpositions that correspond to efficiently integrable probability distributions Lov Grover and Terry Rudolph, quant-ph/0208112
11. Constructing physically intuitive graph invariants Terry Rudolph, quantph/0206068
12. Evolution in time of an N-atom system. II. Calculation of the eigenstates Terry Rudolph, Itay Yavin and Helen Freedhoff, quant-ph/0206067 Phys. Rev. A. 69, 013815 (2004).
13. Quantum searching a classical database (or how we learned to stop worrying and love the bomb) Terry Rudolph and Dr.(Strange)Lov Grover, quant-ph/0206066
14. The laws of physics and cryptographic security Terry Rudolph, quantph/0202143
15. A quantum protocol for cheat-sensitive weak coin flipping Rob Spekkens and Terry Rudolph, quant-ph/0202118 Phys. Rev. Lett. 89, 227901 (2001).
16. Comment on "The Quantum State of a Propagating Laser Field Terry Rudolph and Barry C. Sanders quant-ph/0112020
17. A simple gate for linear optics quantum computing, T. Rudolph and J.-W. Pan, quant-ph/0108056
18. Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol, Rob Spekkens and Terry Rudolph, quantph/0107042 Journal Quantum Information
19. Avatar Tulsi, ”Adiabatic Quantum Computation starting with a 1-D projector Hamiltonian”, Accepted for publication in Phys. Rev. A. quantph/0806.0385.
20. Avatar Tulsi, ”Faster quantum-walk algorithm for the two-dimensional spatial search” , To appear in Phys. Rev. A. quant-ph/0801.0497
21. Avatar Tulsi, ”Quantum computers can search rapidly by using almost any selective transformation” To appear in Phys. Rev. A. quant-ph/0711.4299

22. Fixed-point quantum searching, Lov K. Grover, Physical Review Letters, Vol. 95, Pages 150501, October 7, 2005.
23. Quantum Error Correction of Systematic Errors using a Quantum Search Framework, Ben Reichardt & Lov K. Grover, Physical Review A 72, 042326, October 25, 2005.
24. Preserving Quantum States - A super-Zeno effect, Deepak Dhar, Lov K. Grover, Shasanka Roy, Physical Review Letters, Volume 96, issue 10, March 16, 2006.
25. A new algorithm for directed quantum search, T. Tulsi, L. Grover, and A. Patel, Quantum Information & Computation, Volume 6, No. 6, September 2006.
26. Simple Algorithm for partial quantum search, Vladimir Korepin & Lov K. Grover, Quantum Information Processing, vol. 5, number 1, page 5-10, 2006.
27. Is partial quantum searching of a database any easier? Proceedings SPAA, 2005, Jaikumar Radhakrishnan and Lov K. Grover.
28. Superlinear amplitude amplification, Lov Grover, quant-ph - June 3, 2008

Number of Papers published in peer-reviewed journals: 28.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

(d) Manuscripts

Number of Manuscripts: 0.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Faculty Supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME	PERCENT SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Quantum Search and Beyond

Lov K. Grover, *lkgrover@bell-labs.com*
Bell Laboratories, Lucent Technologies,
1D-435, 600-700 Mountain Avenue, Murray Hill NJ 07974

Abstract

Ten years ago, the quantum search algorithm was designed to provide a way of searching a space of N items in only $\sqrt{N}$ steps. In the last ten years, it has been used as a building block for numerous applications, both physical and algorithmic - these are as diverse as precision measurement and communication complexity. It has been generalized to the amplitude amplification principle in which form it can be used to give a square-root speed-up to almost any probabilistic algorithm. Our research during this period has led to further developments into the applications of quantum searching, including three new variants of quantum searching - partial quantum searching, fixed point quantum searching & super-linear amplitude amplification.

1 Foreword

Folklore is that writing a report is one of the dullest parts of research. This report is turning out to be different. There were tremendous numbers of ideas generated during this period, unfortunately only a fraction of them will ever be written. When reviewing them for writing this report it is very difficult not to get sucked into several hours or even days of research where one reexamines them in the light of the present state of one's knowledge.

This is an exciting time to be in the area of quantum computing. Almost every week sees the emergence of important new applications for quantum computers as well as new designs that would enable their implementation. The emphasis of my research continues to be the former, i.e. to understand and develop the computational power in a quantum computer.

The framework for quantum computation consists of unitary operations. From a computational perspective these are considerably more general than classical computation which mostly consists of the evaluation of boolean functions. Yet, despite this apparent power, only two significant applications have been invented where a quantum computer have a significant advantage over a classical one. The first is factorization and the second is searching.

In 1994, Peter Shor invented an algorithm for factorization. This was exponentially faster than any known classical algorithm and solved a problem that mathematicians and computer scientists had been grappling with for years. This discovery gave a boost to the field and to date remains the most powerful potential application for a quantum computer.

In 1996, I invented the quantum search algorithm. The search algorithm made use of the fact that a quantum system could simultaneously be in multiple states, to search an unsorted database of size N in only $\sqrt{N}$ steps. The quantum search algorithm is perhaps the simplest possible quantum algorithm and because of its simplicity and power it attracted considerable interest from both physicists and computer scientists. It has been proved that no algorithm, whether quantum mechanical or classical, can ever hope to improve quantum search for the application of exhaustive searching. In contrast to factorization which has remained largely a standalone (though very important) application, several algorithmic extensions of quantum search for related applications have been made. It continues to provide a constant source of inspiration in a number of important areas and has by now become an essential part of the toolkit of the quantum computing scientist.

This period saw the development of the class of recursive quantum algorithms. To date most search algorithms had been iterative, during this period we showed the limits of iterative algorithms by developing the fixed point class of quantum search algorithms These are characterized by the property of monotonic convergence which *cannot* be achieved by iterative unitary transformations.

The other important result during this period was that I_0 in the amplitude amplification transformation could be replaced by any transformation R_0, that has the property that only the 0 state is rotated by π radians, all other states

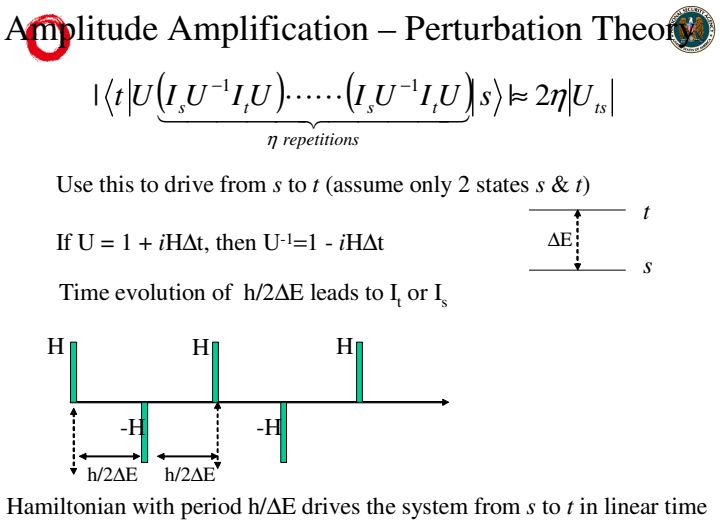

Figure 1: The quantum search algorithm can be looked upon as a resonant perturbation. With this perspective, many of the newer ideas (such as replacing R_0 by a selective rotation that shifts the phase of all states) naturally follow.

should be rotated by an amount that is a finite amount away from π (although this was based on the quantum search algorithm, the breakthrough actually took place due to work by Ambainis et al in the context of the element distinctness problem). This considerably expands the scope of amplitude amplification and has recently led to the development of a large class of random walk algorithms.

A new class of algorithms was proposed in which the amplitude itself rises quadratically with the number of queries. This would be applicable in situations where the initial amplitude in the target state is small.

The other important result during this period was the result demonstrating it is possible to achieve dynamic decoupling by means of appropriately positioned selectively inverting pulses (these selectively inverted the region from which the system was to be insulated.) This was similar in spirit to the quantum search algorithm, the main difference was that the $U^\dagger$ transformation was not available (this is somewhat tangential to our main research and will not be discussed in this report - for more information, see the PRL article in which this appeared - reference 24 in section 6).

There was considerable effort spent on NP-completeness, even though this has not resulted in the desired breakthrough so far, it has helped to develop new ideas. Also, the breakthrough appears to be much closer.

2 Extensions to quantum searching

We have investigated several ways, described below, in which the resources utilized for implementing the quantum search algorithm can be modified, some of these would help bring practical implementation closer.

It has been proved that the quantum search algorithm is the best possible algorithm for the exhaustive search problem. The proof for this bound is complicated and based on subtle properties of unitary transformations. We continue to look for a simpler proof. The proof is rigorous but based on certain assumptions. The question we would like to ask is whether there are ways of working around these assumptions to get a better algorithm. The proofs for the $\sqrt{N}$ bound assumes a decoupling of the oracle from the processing circuitry. The only interaction among the two is whereby the oracle inverts (or does not invert) the phase of the desired states in a superposition [Kas02] have shown that the power of search-related algorithms can depend on the nature of the oracle. It is not clear whether the proofs for the $\sqrt{N}$ bound will hold up for circuits where the oracle gets entangled with the processing circuitry in intermediate steps of computation. We took a close look at the proofs (there are several variants of these) and if we find any loopholes, then try to synthesize circuits that take advantage of these loopholes. Unfortunately, the proofs are very robust - especially the [BBBV] proof that in fact appeared before the search algorithm was discovered.

In classical computation, analog circuits can sometime be more powerful than digital circuits - neural network circuits are one example of such circuits. Is it possible to devise analog circuits that might not be limited by the $\sqrt{N}$ bound? Farhi & Gutmann [Far98] do prove a $\sqrt{N}$ type bound for analog circuits, this proof, though in an analog context, is basically similar to the other proofs. In summary, there have been considerable developments in this direction, most notably the adiabatic search and the random walk algorithms, though they have not originated directly from my own research. This is a sub-field that I am now getting into.

The bounds proved are for the number of queries. What is important is the total number of steps, or the total time, that the algorithm needs. The partial inversion about average scheme provides one example of a scheme whereby one can trade-off additional queries for other processing steps. We continue to look for other such schemes.

The basic $\pi/3$ phase shift quantum search algorithm which was presented in the original paper is well understood though I believe still not adequately enough appreciated by the quantum computing community. Just like the quantum search algorithm took several years after its invention in 1995 for its impact to be fully appreciated, I believe it will take a few years for the $\pi/3$ phase shift quantum search algorithm to be fully appreciated. This algorithm offers a novel framework for error correction which is the dominant problem facing quantum computer implementation. During the year there were a handful of papers on this algorithm (one by Ben Reichardt and myself and the other by two Chinese authors). That is barely indicative of the algorithm's potential - Dan Marinescu

of the University of Central Florida and author of a recent book on quantum computation described it as - "a discovery even more important than the search algorithm".

2.1 Partial Inversion about Average

The quantum search algorithm works by repeating an alternating sequence of operations, the first is an inversion about average operation and the second is a selective phase inversion. The inversion about average step needs to be done in the Fourier domain and it requires transforming back and forth from the current to the Fourier domain. The Fourier domain in this case is the Walsh-Hadamard domain and it requires as many qubit operations as the qubits required to represent the data. The partial inversion about average technique shows that it is not necessary to Fourier transform all the qubits in each step - in fact if there are N states, and therefore $\log N$ qubits, it is just necessary to transform $\log(\log N)$ qubits. The price paid for this was a slight increase in the number of queries (the quantum search algorithm is known to be optimal in terms of queries and so any changes to the algorithm is almost certain to lead to an increase in the number of queries). The algorithm this leads to is quite different from the search algorithm and is likely to have other consequences [Gro02b].

2.2 $\pi/3$ phase shift quantum searching

The original quantum search algorithm is known to be the best possible algorithm for exhaustive searching therefore no algorithm will be able to improve its performance. However, for applications other than exhaustive searching for a single item, suitably modified algorithms may indeed provide better performance. For example if we consider the problem of searching N items when there are either one target items or two target items with equal probability, the problem suddenly goes from a well understood problem to an open problem. It is in this realm when there is uncertainty in the problem parameters, does the new framework of $\pi/3$ phase shift quantum searching, prove most useful.

2.3 Fixed point quantum searching

It was generally believed that iterative quantum transformations could not have fixed points. This is because quantum transformations are unitary and thus have eigenvalues with absolute value equal to unity. Therefore any iterative quantum procedure would have to be periodic and would not be able to have fixed points. There are two ways round this intrinsic limitation - (i) modify the iterative nature of the procedure so that the iterations in successive steps are slightly different, (ii) incorporate measurements in the intermediate steps (so that the procedure is no longer unitary). I invented the first fixed point quantum search algorithm which attained its fixed point nature by having slightly different unitary operations in each iteration - this variation in unitary transformations follows naturally by concatenation of $\pi/3$ phase shifts.

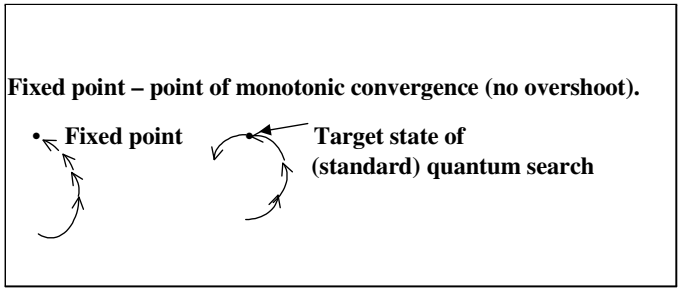

Figure 2: Fixed-point quantum search algorithms converge monotonically to the solution, whereas the standard quantum search algorithm overshoots the target state, if the number of iterations is more than the optimal number.

Unlike the amplitude amplification transformation, it is not possible to iterate the transformation $UR_sU^\dagger R_tU\ |s\rangle$ to obtain larger rotations of the state vector in a carefully-defined two dimensional Hilbert space (the behavior of an iterated sequence will be quite different). However, it can be obtained by recursion as follows. The basic idea is to define the transformation U_{m+1} by the recursion:

$$U_{m+1} = U_m R_s U_m^\dagger R_t U_m, \qquad U_0 = U. \tag{1}$$

Unlike amplitude amplification, it is *not* simple to write down the precise operation sequence for U_m with large m without working out the full recursion. Recursion for each m is different and there is no simple structure. Let us illustrate this for U_2:

$$\begin{aligned} U_0 &= U, \qquad U_1 = U_0 R_s U_0^\dagger R_t U_0 = U R_s U^\dagger R_t U \\ U_2 &= U_1 R_s U_1^\dagger R_t U_1 = \left(U R_s U^\dagger R_t U\right) R_s \\ &\qquad\qquad \left(U R_s U^\dagger R_t U\right)^\dagger R_t \left(U R_s U^\dagger R_t U\right) \\ &= U \left(R_s U^\dagger R_t U\right) \left(R_s U^\dagger R_t^\dagger U\right) \left(R_s^\dagger U^\dagger R_t U\right) \left(R_s U^\dagger R_t U\right) \end{aligned} \tag{2}$$

The corresponding transformation for amplitude amplification is:

$$U \left(I_s U^\dagger I_t U\right) \left(I_s U^\dagger I_t U\right) \left(I_s U^\dagger I_t U\right) \left(I_s U^\dagger I_t U\right) \tag{3}$$

Note that in (2), the sequence repeated in each iteration is slightly different due to the presence of the four operations $R_s, R_t^\dagger, R_s^\dagger, R_t$. Therefore, we are able to circumvent the condition regarding repetition of identical unitary operators that prevented amplitude amplification from having a fixed point.

It came as a big surprise that there existed a second algorithm (based on measurements) that attained its fixed point by an entirely different mechanism, yet had the same worst case behavior as the previously discovered unitary fixed point algorithm (this is described in the 2006 interim report).

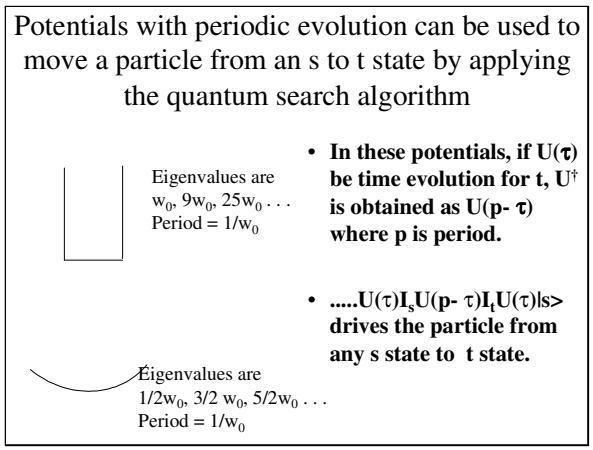

Figure 3: The quantum search algorithm results in a natural scheme to move particles in certain kinds of potential wells.

2.4 Fixed point quantum *computing*

As mentioned in the previous section, the fixed-point quantum searching algorithms lead to "probability-like" behavior, i.e. their behavior is somewhere between quantum and classical. This is significant because it may help us overcome some of the limitations imposed by quantum computation while preserving the benefits. An example is moving a particle in a harmonic oscillator potential.

As shown in the diagram below, the particle may start from various initial reaches the same final state at the end of the sequence of operations. This in itself is not so surprising since the quantum search algorithm does accomplish this, e.g. in the amplitude amplification transformation, the source states and the target states can be arbitrary, i.e. if we repeat the amplitude amplification transformation the appropriate number of times, we reach the target state. However this is subject to the constraint that we stop at the right time and this time depends on the initial state, i.e. the number of iterations is $O\left(\frac{1}{\|U_{ts}\|}\right)$ which clearly depends on the source state. What is surprising is that the particle reaches the specified final state regardless of the magnitude of $\|U_{ts}\|$ provided the number of iterations is sufficiently high. Note that unlike regular amplitude amplification, it does not improve the probability of success in each iteration but at the end of the sequence of iterations, the probability can be shown to increase monotonically irrespective of the starting state.

This can be achieved in any potential in which the movement of the particle is periodic, i.e. if the period be p, then if U represent the evolution of the particle for a time τ, the $U^\dagger$ is obtained by evolving the particle for a time $(p-\tau)$.

This holds for two important potentials - the harmonic oscillator potential

and the infinite square well potential where the separation of the eigenfrequencies is by multiples of the lowest eigenfrequency.

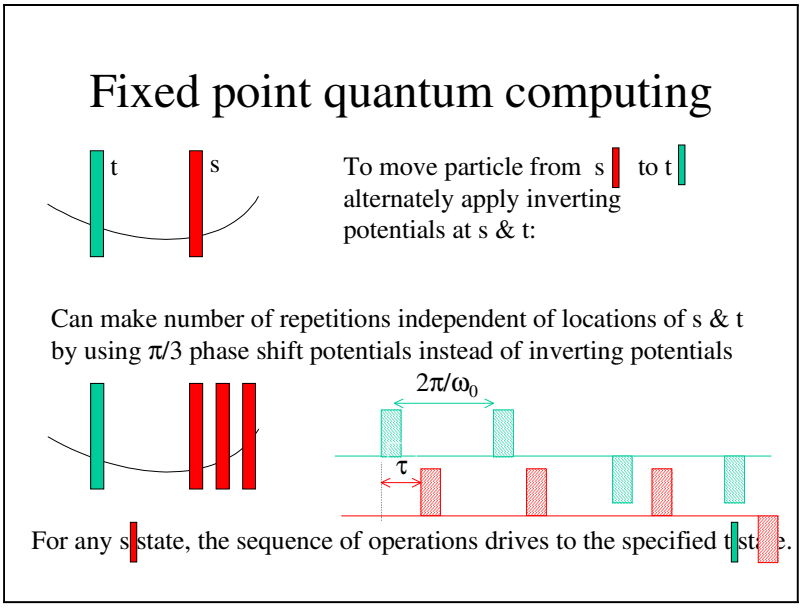

Figure 4: The scheme shown in the previous figure is designed to move a particle between two specific points in the larger potential well. This figure shows how to move it such that it moves between any two arbitrary points, s & t.

2.5 Physical applications of quantum searching - cavity design

Cavity design has become an important problem after the advent of lasers since the cavity plays such a critical role in the performance of the laser and this problem has been well studied (actually even though for concreteness we will talk in terms of optical cavities, the principle is applicable to any kind of distributed resonator). There are several ways to analyze and design cavities using either ray optics or wave optics in the paraxial approximation. In either of these techniques, the structure is made to satisfy the condition that it reproduce itself after a round-trip. This condition may be shown to be necessary in a one-dimensional structure; in higher dimensions (two & three) it is sufficient but not necessary (e.g. whispering gallery modes), we make use of this degree of freedom in this paper by presenting a new class of resonators that utilize transverse variations of the cavity.

Our inetrim report of 2006 describes this in detail, so we will refer the interested reader to that report for details. After that we carried out simulations of

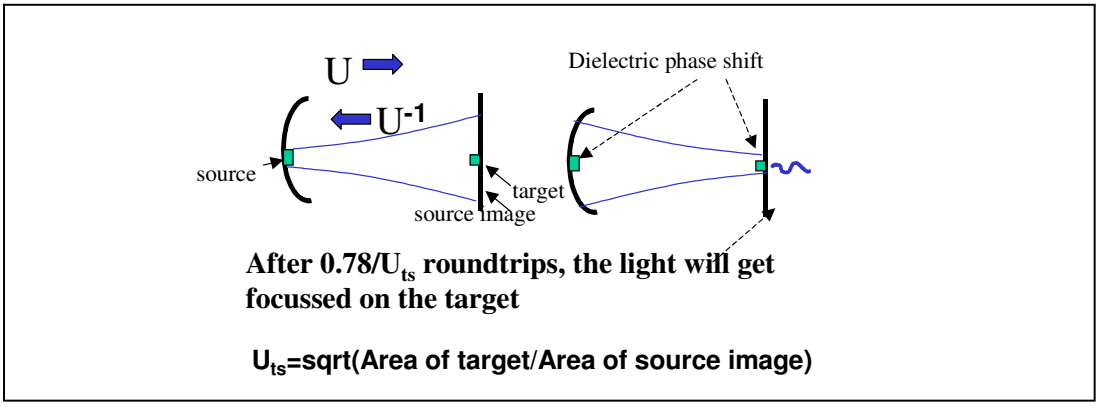

Figure 5: By interspersing the U & $U^\dagger$ operations with selective phase inversions, we obtain the amplitude amplification transformation. As this is iterated, the amplitude in the target state amplifies.

a confocal resonator configuration. This consisted of:

- verifying that a laser pulse that started off from one mirror indeed evolved as predicted by the amplitude amplification framework.
- The eigenvectors of the system were indeed combinations of $|s\rangle$ and $U^\dagger |t\rangle$.
- If the phase inversions were replaced by $\pi/3$ phase shifts, then a pulse that started out at the phase-shift position at one mirror got *monotonically* focussed at the other mirror. Note that by monotonically we mean that the more the iterations the system is designed with, the more accurately it will focus at the target mirror. The systems that would have to be designed with different number of bounces will be quite different as the phase shifts in each bounce will be different.

Note that as expected by an eigenvector analysis of quantum search for the 1 in 4 problem, the two eigenvectors are $\pi/4$ displaced from the base states.

2.6 Multiparty scheduling

A natural application area where quantum computing might be expected to give an advantage is the field of distributed computing since it has been known since the time of Einstein that quantum mechanics leads to non-local paradoxical effects (physicists sometimes call this "spooky action at a distance").

Spatial searching is the problem where there are N parties that are physically separated in space and the problem is to locate the party that has a 1. Through a series of local operations that consist of selective inversions and neighbor to neighbor communications, Aaronson's spatial search paper showed

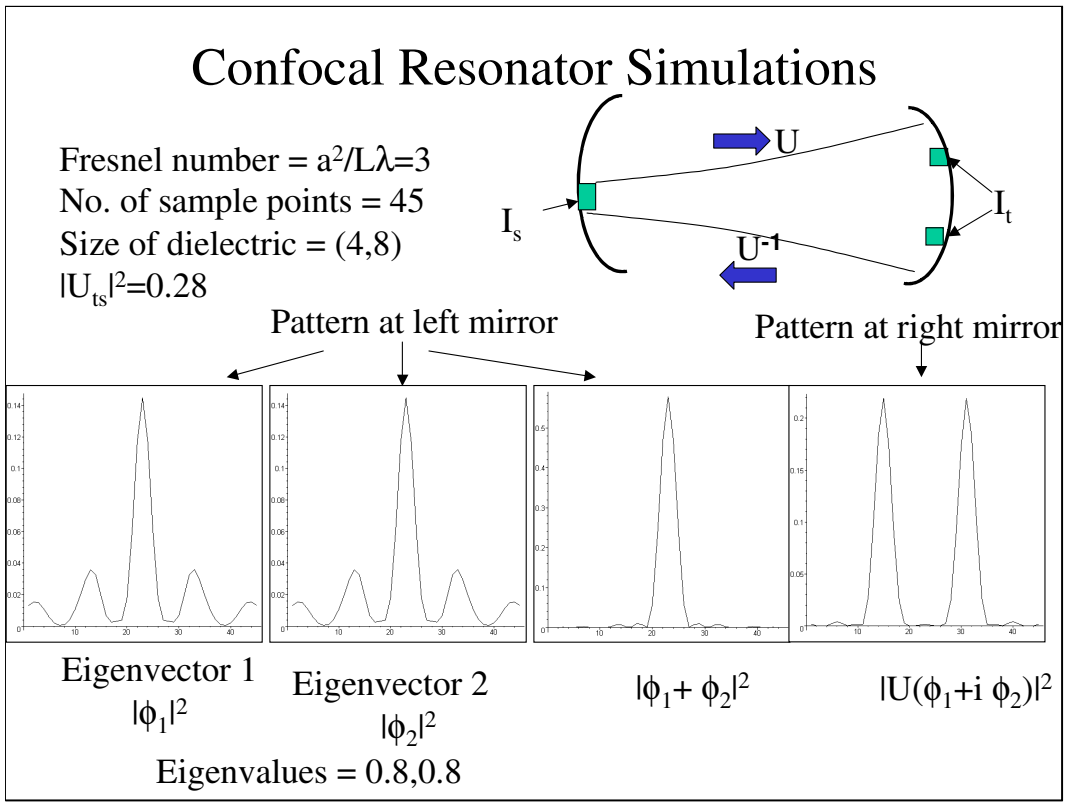

Figure 6: The technique described in this report can be used to tailor the modes of a confocal resonator.

how to locate the site that has a 1. They showed how to do this when the interconnect structure was a lattice of dimension greater than or equal to 2 with only $\sqrt{N}$ communication. This paper makes use of a similar recursive approach, though we can do things much more simply, since we do not bother with log factors and also have the $\frac{\pi}{3}$ phase shift algorithm available which was not known at the time.

In the algorithm of this paper, we set the register into a superposition of all dates, different elements of the superposition do separate quantum random walks on the same graph - the net effect of which is to invert the phase of the dates that are satisfactory to all parties.

This is alternated with an inversion about average which increases the amplitude in these inverted states.

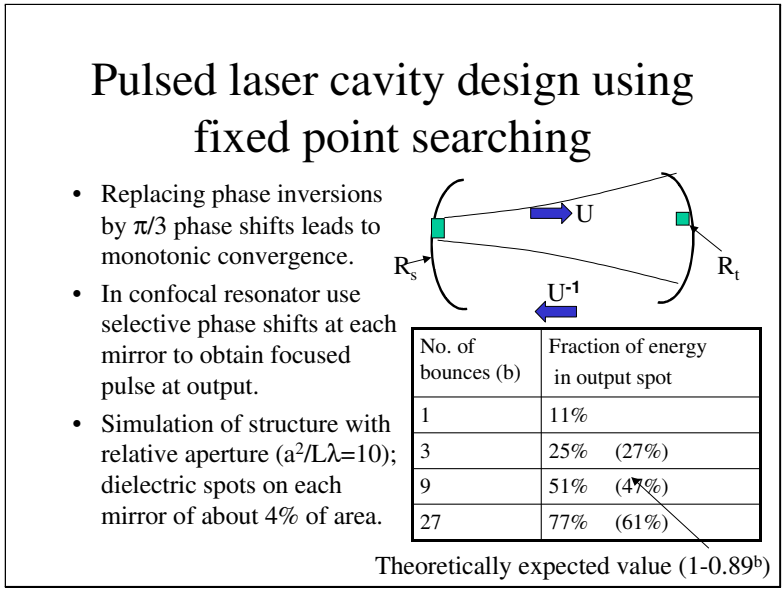

Figure 7: The fixed point technique of quantum search naturally leads to a scheme for focussing a pulse to a target location in the output mirror.

2.6.1 The problem

The two-party scheduling problem is the following: Alice & Bob are two parties that are physically separated. Each has a well defined appointment schedule, the problem is to find a time slot when each of them is available. This is clearly equivalent to the problem of finding a common 1 in two remotely located N bit strings. Classically, they need at least $O(N)$ bits of communication. It was somewhat of a breakthrough when it was shown that quantum mechanically it could be achieved in only $O\left(\sqrt{N}\right)$ qubits of communication by using a distributed quantum search (BCW). This was the first example of an important communication complexity problem where quantum communication gave a significant speedup. This was subsequently proved to be optimal by Rasbarov.

This paper solves the problem of multi-party scheduling, i.e. when multiple (say n) remotely located parties have to agree on a mutually available date out of N possible dates. The obvious quantum algorithm is to extend the BCW algorithm so that at each step a date is considered satisfied if all parties are satisfied. This will take $O\left(\sqrt{N}\right)$ iterations but each step will require O(n) communication, the following algorithm reduces the communication to $O\left(\sqrt{Nn}\right)$.

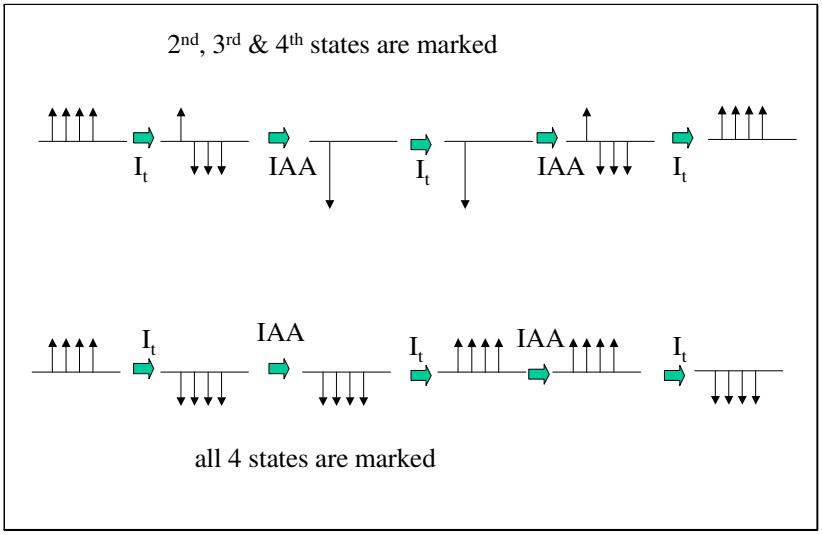

Figure 8: In a 4-state system, there are either 3 marked states or all 4 marked states. The sequence of 3 selective inversions of marked states (I_t) and two inversion about average transformations (IAA) will invert the amplitude only in the case of all 4 marked states.

2.6.2 Outline of approach

The following section illustrates the scheme of the algorithm in step-by-step detail. Although, the amount of communication required in this case is not significantly better than other quantum algorithms, the asymptotic scaling is much better as described in the following sections.

The algorithm of this section makes use of the following feature of a four-state system. If a function evaluates to 1 either on three of the four states and 0 on the fourth, or 1 on all four of the states, then an alternating sequence of three selective inversions and two inversions about average operations will invert the phase of a uniform superposition in the case the function evaluates to zero in all four states, in case the function evaluated to 1 only on three states, it leaves the uniform superposition unchanged.

Figure 7 illustrates the approach of this algorithm on a structured problem where there are four parties, either three or all four are satisfied with a particular date, furthermore there are eight possible dates and all the parties are satisfied on two of these dates. Start with two registers, the first is initialized to a superposition of all dates and the second to a superposition of all parties, i.e. the initial state is $(|A\rangle+|B\rangle+|C\rangle+|D\rangle)\otimes(|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle+|8\rangle)$ (we ignore the normalization constant).

The date register is next sent to the party indicated by the party register. This party, if it is satisfied with that date, inverts the phase and sends it back.

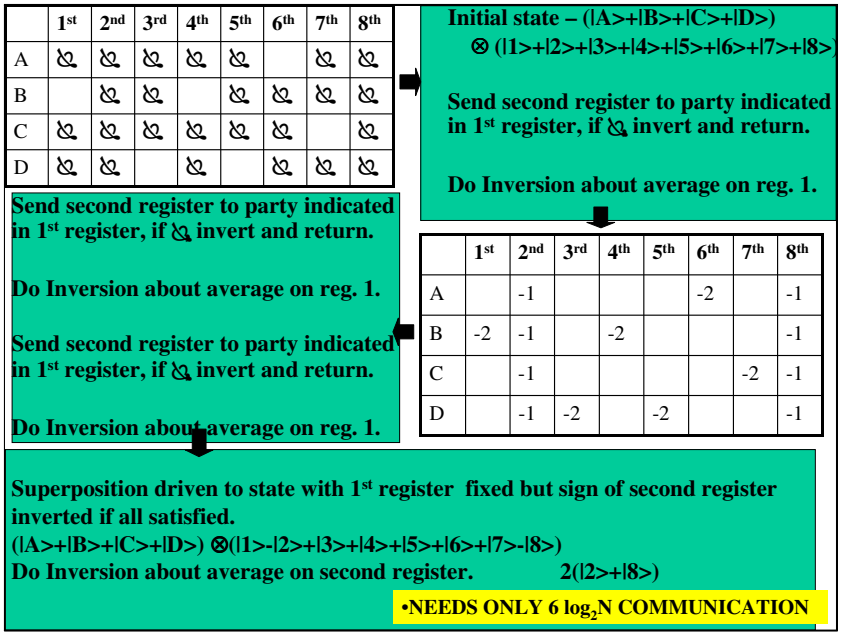

Figure 9: This example illustrates the scheme of the algorithm. In three round-trips of the register S one can find a suitable slot.

The superposition becomes:

$$
\begin{aligned}
&(-|A\rangle + |B\rangle - |C\rangle - |D\rangle) \otimes |1\rangle \\
&+(-|A\rangle - |B\rangle - |C\rangle - |D\rangle) \otimes |2\rangle \\
&+(-|A\rangle - |B\rangle - |C\rangle + |D\rangle) \otimes |3\rangle \\
&+(-|A\rangle + |B\rangle - |C\rangle - |D\rangle) \otimes |4\rangle \\
&+(-|A\rangle - |B\rangle - |C\rangle + |D\rangle) \otimes |5\rangle \\
&+(|A\rangle - |B\rangle - |C\rangle - |D\rangle) \otimes |6\rangle \\
&+(-|A\rangle - |B\rangle + |C\rangle - |D\rangle) \otimes |7\rangle \\
&+(-|A\rangle - |B\rangle - |C\rangle - |D\rangle) \otimes |8\rangle
\end{aligned}
$$

An inversion about mean on the first register drives it into the states which are not satisfied on that particular date - except in the case when all parties are satisfied.

$$
\begin{aligned}
&-2|B\rangle \otimes |1\rangle + (-|A\rangle - |B\rangle - |C\rangle - |D\rangle) \otimes |2\rangle - 2|D\rangle) \otimes |3\rangle - 2|B\rangle \otimes |4\rangle \\
&-2|D\rangle \otimes |5\rangle - 2|A\rangle \otimes |6\rangle - 2|C\rangle \otimes |7\rangle + (-|A\rangle - |B\rangle - |C\rangle - |D\rangle) \otimes |8\rangle
\end{aligned}
$$

Next we repeat this sequence of selective inversions and inversions about mean one more time and after that do a final selective inversion. As indicated in the beginning of this section, the net effect of the three selective inversions and two inversion about averages is to invert the phase if all parties are satisfied. The superposition may now be written in the form $(|A\rangle + |B\rangle + |C\rangle + |D\rangle) \otimes (|1\rangle - |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle - |8\rangle)$.

A single inversion about average on the date register will drive it into dates corresponding to states where all parties are satisfied.

It has recently been realized that this is equivalent to an AND of ORs which can be carried out by standard quantum searching. The problem is equivalent to an OR of n ANDs, each of which is over N variables. Using the basic search algorithm recursively, you can do this in $O\left(\sqrt{Nn}\right)$ queries in the black-box model. (Eliminating a log factor involves the recursive algorithm due to Hoyer, Mosca and de Wolf from ICALP 2003.)

This realization has prompted us to look for further novel applications of our framework. One application is when we need to find the best schedule, which may not be the perfect schedule. In this situation in each iteration of the inner loop, we do a counting (this can be carried out by the Valiant-Vazirani algorithm which consists of sampling followed by successive bisection of the graph) and in the outer loop instead of an AND we do a minimum using the Hoyer-Durr adaptation of the quantum search algorithm. This cannot be implemented by a simple AND-OR circuit.

2.7 Superlinear Amplitude Amplification [1]-

Quantum search/amplitude amplification algorithms are designed to be able to amplify the amplitude in the target state linearly with the number of operations. Since the probability is the square of the amplitude, this results in the success probability rising quadratically with the number of operations. This section presents a new kind of quantum search algorithm in which the amplitude of the target state increases quadratically with the number of operations. However, the domain of applications of this is much more limited than standard amplitude amplification.

Quantum searching was invented to speed up the searching process in databases. It was realized by Hoyer et al [[**?**]]and independently by me [[**?**]] that this searching was a special case of amplitude amplification whereby the amplitude in a target state could be amplified linearly with the number of operations. This realization considerably increased the power of the algorithm, no longer was it limited to database searching but was applicable to a host of physics and computer science problems. In fact it gave a square-root speedup for almost any classical probabilistic algorithm.

The idea behind this speedup was realized later on to be a two dimensional rotation through which the state-vector got driven from the source to a target state through a sequence of small rotations in the two dimensional space defined by the source and the target state.

This is easily seen by considering the basic transformation: $-UI_sU^{-1}I_tU$ say V. Then if we calculate V_{ts}, by definition of the I_t & I_s operations, it easily follows that

$$V_{ts} = (-UI_sU^{-1}I_tU)_{ts} = 3U_{ts} - 4\left|U_{ts}\right|^2 \approx 3U_{ts} \tag{4a}$$

Note that this is true for any unitary U. It stays true if we replace U by V which yields:

$$(-VI_sV^{-1}I_tV)_{ts} = 3V_{ts}$$

Substituting for V as $-UI_sU^{-1}I_tU$ in (5) and V_{ts} from (4a), it follows that:

$$(-UI_sU^{-1}I_tUI_sU^{-1}I_tUI_sU^{-1}I_tUI_sU^{-1}I_tU)_{ts} \approx 9U_{ts}$$

Similarly by recursing multiple times, we can prove the transformation: $U(-I_sU^{-1}I_tU)^p_{ts} \approx (2p+1)U_{ts}$ to be true for large p.

2.7.1 Quadratic Amplitude Amplification

This paper gives a new kind of amplitude amplification in which the amplitude in the target grows ;quadratically with the number of iterations. Instead of choosing the basic transformation to be $V = -UI_sU^{-1}I_tU$, we choose V to be $-U^{-1}I_tI_sU$. It follows by using the definitions of I_s & I_t, that

$$V_{ts} = \left(-U^{-1}I_tI_sU\right)_{ts} = 2U_{ss}U^*_{ts} + 2U^*_{tt}U_{st} \tag{5}$$

[1] This topic is discussed in somewhat greater detail since it is based on a very recent result, one that most readers may not be familiar with.

In case $U_{ss} \approx U_{tt}^*$ and $U_{st} \approx U_{ts}^*$, then $V_{ts} \approx 4U_{ss}U_{ts}$.Unlike the recursion equation of the previous transformation which only depended on U_{ts}, this equation depends on both U_{tt} and U_{ss} and even U_{st}. So we need to investigate how U_{tt} and U_{ss} vary in successive recursions.

Consider V_{ss}. Again assuming $U_{st} \approx U_{ts}^*$ and $U_{ss} \approx U_{tt}^*$

$$V_{ss} = \left(-U^{-1}I_tI_sU\right)_{ss} = -1 + 2\left|U_{ss}\right|^2 - 2\left|U_{ts}\right|^2$$

Note that if we denote $U_{ss} = (1-\delta)$, and V_{ss} by $(1-\gamma)$ assuming all terms to be real and neglecting $2\left|U_{ts}\right|^2$ on the RHS, the above equation may be written as:

$$\gamma \approx 4\delta$$

Therefore V_{ss} stays close to 1 for approximately$\frac{\ln\frac{1}{\delta}}{\ln 4}$ recursions. In i recursions, provided $U_{tt} \approx 1$, U_{ts} rises by a factor of approximately 4^i; therefore in $\frac{\ln\frac{1}{\delta}}{\ln 4}$ recursions U_{ts} rises by approximately a factor of $\frac{1}{\delta}$. The number of queries is approximately $2^{\left(\frac{\ln\frac{1}{\delta}}{\ln 4}\right)}$ which is $\frac{1}{\sqrt{\delta}}$, as expected the amplification of U_{ts} is quadratic in the region when U_{ss} is approximately 1.

2.7.2 Example - U is the Inversion about Average Operation

Consider the situation when s, the starting state is an arbitrary basis state and U is the inversion about average transformation. Then, assuming there to be N states to be searched, U_{ss} is $-1+\frac{2}{N}$ and U_{ts} is $\frac{2}{N}$. Then analyzing the sequence of operations for a few steps-

- $U = WI_0W$
- $-U^{-1}I_tI_sU = -\underbrace{WI_0W}\ I_tI_s\underbrace{WI_0W} = W\ I_0\ W\ (I_tI_s)\ W\ I_0\ W$
- $$\begin{aligned} U^{-1}I_tI_sU\ I_sI_t\ U^{-1}I_tI_sU &= \underbrace{WI_0W}\ I_tI_s\underbrace{WI_0W}\ I_sI_t\ \underbrace{WI_0W}\ I_tI_s\underbrace{WI_0W} \\ &= \cdots W\ I_0\ W\ (I_tI_s)\ W\ I_0\ W\ (I_tI_s)\ W\ I_0\ W \end{aligned} \quad (6)$$

Looks something like the search algorithm, which is:

$$= \cdots W\ I_t\ W\ I_t\ W\ I_s\ W\ I_t\ W\ I_s\ W$$

However, any similarity is superficial, as we discuss in the following section, this algorithm is *not* a rotation of the state vector in two-dimensional Hilbert space.

Nevertheless, the dynamics of the algorithm are fairly simple to understand and analyze iteratively: The state just before an inversion about average is

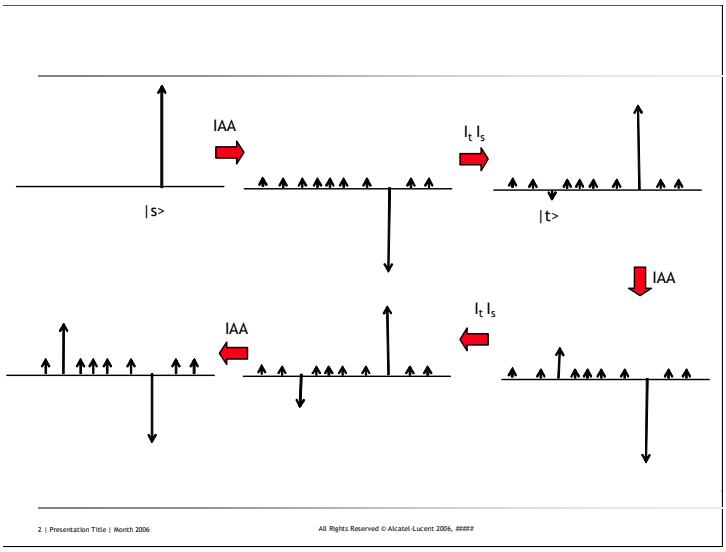

Figure 10: This describes two iterations of the new quantum search algorithm. As described above, the U transform is the Inversion about Average operation (IAA).

described by 3 parameters, the amplitudes in the target state, source state and that in the other states.

The evolution is obtained by the following equations (A(t) denotes the average amplitude over all states):

$$\begin{aligned} .\Delta A(t) &= 2\frac{S(t)}{N} - 2\frac{T(t)}{N} \\ \Delta S(t) &= -2A(t) \\ \Delta T(t) &= 2A(t) \end{aligned}$$

Going to the continuous limit and solving this system of differential equations gives the amplitude in the target state as $\frac{1}{2} - \frac{1}{2}\cos\left(\frac{2\sqrt{2}t}{\sqrt{N}}\right)$. Therefore in $t = \frac{\pi\sqrt{N}}{2\sqrt{2}}$ iterations, the amplitude in the target state becomes unity.

2.7.3 Observations

The number of iterations required for searching with certainty is $\sqrt{2}$ times more than required by the search algorithm.

The variation of the amplitude in the target state is $\frac{1}{2} - \frac{1}{2}\cos\left(\frac{2\sqrt{2}t}{\sqrt{N}}\right)$. in the initial stages (when t is close to 0), the amplitude varies as $\frac{2t^2}{N}$As

expected, the rate of increase is quadratic. However, once the probability in the target state become significant (also affecting U_{ss}), the quadratic nature of the increase is destroyed.

The algorithm of this paper may be useful in applications where the basic U_{ts} that needs to be amplified is small (in the above example where the U transform was the inversion about average, U_{ts} was only $\frac{2}{N}$ - whereas in the search algorithm it is about $\frac{1}{\sqrt{N}}$.

It is possible that there would exist applications where a few applications of this algorithm provided the driving transform for amplitude amplification algorithms. That way, we would get the quadratic speedup plus the flexibility of the amplitude amplification algorithms.

2.7.4 This is not the search algorithm

One might be tempted to conclude that the above algorithm was a variant of the search algorithm because, overall, it gave a square-root speedup; also it consists of similar sequences of unitary transformations (6). However, that is not the case.

The chief characteristic of the search algorithm and all its variants (amplitude amplification algorithms) was a rotation of the state vector in appropriately defined two dimensional space. The algorithm of this paper needs more than two dimensions to operate in. To see this consider the basic recursion equation (5) used to develop the algorithm: $V_{ts} = \left(-U^{-1} I_t I_s U\right)_{ts} = 2U_{ss}U^*_{ts} + 2U^*_{tt}U_{st}$. Given large U_{ss} & U_{tt} and $U_{st} \approx U^*_{ts}$, we had argued that V_{ts} was amplified significantly in each recursion. In order to satisfy this condition needs more than two dimensions. This is because if there were only two dimensions it would follow from unitarity of U that $2U_{ss}U^*_{ts} + 2U^*_{tt}U_{st}$=0 (any two columns of a unitary matrix are orthogonal) - therefore, additional dimensions are necessary.

2.7.5 Summary of superlinear amplitude amplification

The above algorithm gives a quadratic amplification under certain conditions. The quadratic amplification offers something new beyond the search algorithm, even though it is not as universally applicable. To borrow a term from analog amplifiers: this only has a limited dynamic range - outside of this range it has to be supplemented by other more robust algorithms.

Just as the amplitude amplification principle, quantum searching and fixed-point quantum searching, this algorithm provides yet another tool in the quantum algorithm designer's toolkit. Whereas, amplitude amplification and quantum searching are independently useful to design quantum algorithms, the fixed point algorithms & the algorithm of this paper may be useful in combination with other algorithms - fixed point algorithms to improve the robustness and the algorithm of this paper to increase the amplification in selected ranges.

As described in the *Observations* section, the algorithm of this paper may be useful in conjunction with the standard quantum search algorithm. This is

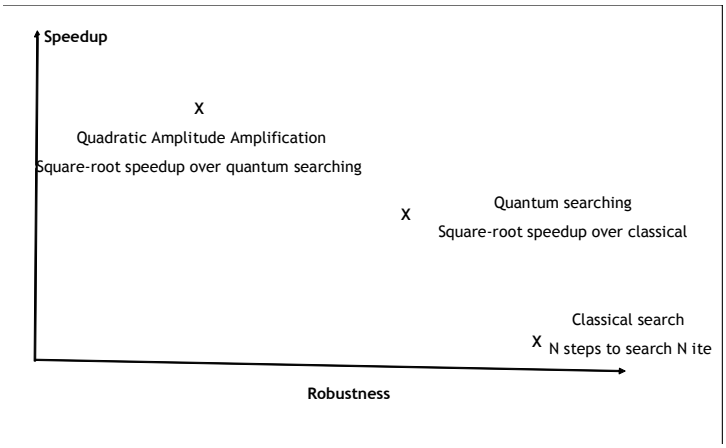

Figure 11: Hierarchy of search algorithms - The quantum search algorithm attained a square-root speedup over classical but the price paid was more sensitivity. The present algorithm provides a square-root speedup over quantum searching, but it still more sensitive.

somewhat similar in spirit to applications where the search algorithm is combined with a classical algorithm. One such example is the counting algorithm of [Bra98] where one gets round the cyclical nature of the search algorithm by making appropriately timed observations (which is the classical algorithm). The counting algorithm is not usually looked at this way, but in the context of robustness versus speed, it is insightful to look upon it as a combination of classical and quantum search algorithms,

2.8 Using incoherent ancillas

We have noticed that a modified quantum search algorithm works almost the same as the original algorithm if the phase inversion step is replaced by a counting step in which a quantum device counts how many times the system has passed through the solution state. The advantage with such a structure is that it does not need to maintain phase matching with the rest of the structure. In fact, we have found using density matrix calculations that the algorithm still works even if the counter is not totally coherent.

We also find that this version of the search algorithm, while requiring an increase in the number of oracle queries (by only a constant factor) is much more stable with respect to overshooting/undershooting the optimal number of queries. We are thinking of applications where this observation would give a decisive advantage over the standard search algorithm.

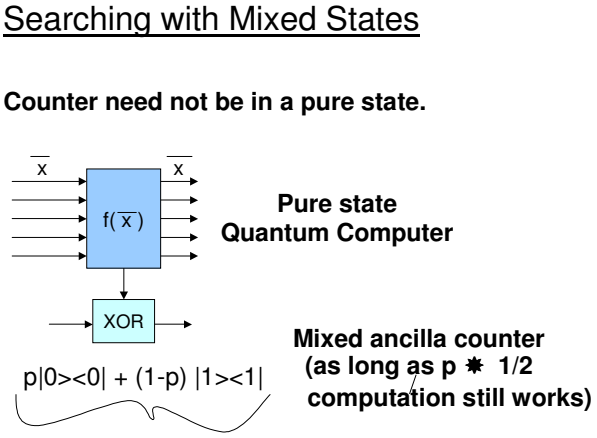

Figure 12: The phase inversion module of the quantum search algorithm can be replaced by a counter. Such a system is much less sensitive to perturbations.

2.9 Incoherent versus coherent qubit interactions: Subspace projection as a computational primitive

Performing universal quantum computation is generically equated with the ability to build up arbitrary unitary transformations on a large number of qubits out of a set of unitary transformations that act on a small number of qubits at a time. As such, the primary challenge of building a quantum computer is most often considered to be finding quantum systems with appropriately controllable Hamiltonians, such that the desired unitary evolution is obtained to within some small error.

While this standard paradigm certainly enables universal quantum computing, recent results have shown that it is not necessary that the computation be built up in such a way. In particular it has been shown that we can often replace the 'hard' parts of a quantum computation (generally the 2 qubit interaction) by using measurements and appropriately prepared ancilla states. In particular, Gottesman and Chuang [Got99]showed that teleportation is such a universal computational primitive. Recently some beautiful ideas for implementing quantum computation by performing measurements on appropriately prepared ancilla states have been presented [Rau01, Nie01]; these latter schemes are remarkable in that they require no coherent (unitary) evolution during the computation at all.

By coupling an idea of Paul Kwiat's with an idea of ours (which originated in the work on quantum searching a classical database, Section 2.3), we have

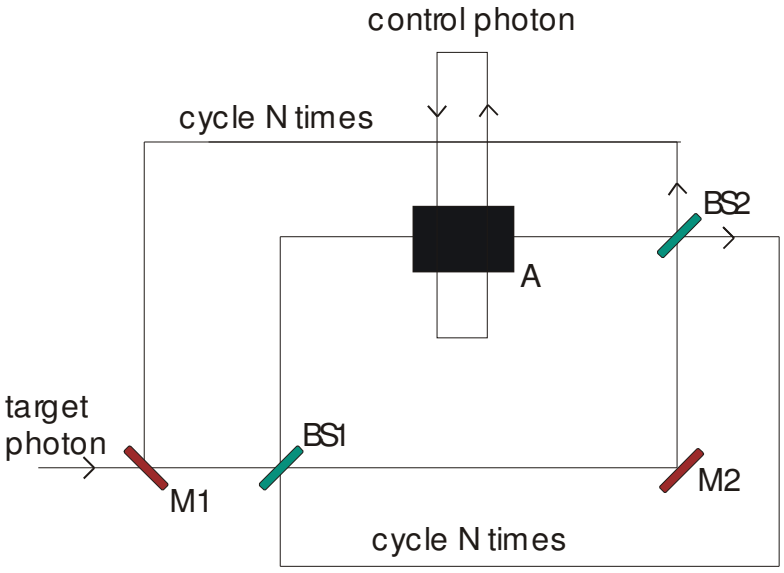

Figure 13: It is possible to use an absorbing process to achieve quantum computation using interaction-free measurements.

shown that a two outcome projective measurement

$$P_1 = |0\rangle\langle 0| + |1\rangle\langle 1|, P_2 = I - |0\rangle\langle 0| + |1\rangle\langle 1| = \sum_{n=2}^{\infty} |n\rangle\langle n|$$

on a single harmonic oscillator mode can act as quantum computational primitive, which, along with easily implemented single qubit unitary transformations, enables us to perform universal quantum computation. In contrast with the aforementioned schemes, we need make no use of prepared ancilla states. Instead we use the quantum zeno effect in such a way that a series of measurements approximate a useful unitary evolution.

As an abstract mathematical result this is perhaps not particularly interesting. However our scheme allows for the P_2 outcome to be destructive - that is, it absorbs the quanta involved. This is somewhat surprising, since one normally expects that such processes will result in loss of the quantum systems which are being used in the computation.

Fig. 13 is a schematic showing how to use an interaction free measurement to turn the incoherent projective measurement P_1, P_2 into a coherent gate. The black box labelled A consists of a balanced Mach-Zender interferometer, with a measurement of P_1, P_2 in both of its arms. (If two photons are incident on a beamsplitter then the output state is $|2,0\rangle + |0,2\rangle$. Thus a measurement of P_1, P_2 in both outputs will certainly give the absorptive outcome P_2 in one output. If

one photon, or the vacuum, is initially present then the non-destructive outcome P_1will occur in each arm. In effect the box A absorbs the target photon if and only if the control photon is present.) The target photon enters at the switchable mirror M1. It passes through a weakly reflecting beam splitter, of reflectivity $\sin^2\theta = \pi/N$. If the control photon is present, then it collapses onto the path which doesn't contain A; if the control photon is not present then the target proceeds through the interferometer coherently. The photons are cycled N times; by choosing N large enough we can make the probability of failure as small as we wish. It can be shown that this process implements the following two qubit gate:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

This gate coupled with single qubit transformations suffices for quantum computing.

Thus our results show that *absorptive* nonlinear processes can be used to perform useful quantum computation.. As a simple example of why this can be of practical significance, let us think for the moment in terms of photonic qubits. The interaction strength between two photons is very weak (of order $\frac{1}{137^8}$), unless we make use of some nonlinear media. Even with such a medium however, if we limit our considerations to non-resonant (dispersive) interactions then they are still not particularly strong. The primary reason we would limit ourselves to non-resonant interactions however, is simply that resonant ones (which are orders of magnitude stronger) are going to cause absorptive loss of the photons with which we are trying to compute. However using our scheme, although the interaction is incoherent, they are not lost to the computation.

Although phrased in terms of photons, our ideas apply quite generally. As such, we are currently working with our experimentalist colleagues at Bell Labs to think of systems in which strong nonlinear effects are observed at the single quantum level. Almost any system with a strong nonlinearity will suffice.

This ideal led to the (now) well known scheme by Terry Rudolph to carry out robust error correction using a cluster architecture.

2.10 Extended party quantum information processing

The field of quantum information theory can be broadly segregated into two areas of study: (i) *local* information processing (e.g. quantum computation algorithms) and (ii) *extended* quantum information processing (e.g. key distribution, two-party protocols, data hiding, communication complexity, entanglement properties). As in classical information theory, results in one area often yield insights into the other; this forms much of the motivation for studying classical communication complexity for example. In the quantum world the link is, in some sense, much stronger: the power of quantum mechanics for both local

and extended information processing lies ultimately in the tensor product structure of the theory, a structure which it is most natural to probe by considering extended processes. When considering parties engaged in extended quantum information processing, we need to initially specify the resources available to the parties, such as the amount of shared prior entanglement, the characteristics of any classical or quantum channels and so on. A primary part of the study of extended quantum information processing involves examining the achievable tasks under various restrictions in the available resources.

2.10.1 Quantum Communication Complexity

Classical communication and computation have been intricately linked since the time of Shannon. It is well known that appropriate coding can greatly facilitate the transmission of data. Similarly, distributing computation among multiple computers can expedite the solution of certain problems for which the communication needs do not dominate. A similar situation prevails in the quantum world. Quantum teleportation and quantum cryptography all make use of the same concepts and framework as quantum computation. Indeed the quantum technique that gives the best known improvement in communication complexity as compared to classical, consists of an application of the quantum search algorithm in a distributed setting to solve the intersection problem.

I recently discovered an improved algorithm for the intersection problem. This problem consists of finding a common 1 in two remotely located N bit strings. Denote the number of 1s in the string with the fewer 1s by ϵN. Classically, it needs at least $\Omega(\epsilon N \log_2 N)$ bits of communication to find the common 1. The best known quantum algorithm (also based on quantum searching) would require $O(\sqrt{N} \log_2 N)$ qubits of communication. My algorithm improves this to $O(\sqrt{\epsilon N} \log_2 N)$ qubits.

For the last several months, Terry Rudolph and I have been working intensely in the area of quantum communication complexity. We have been trying to see what classical computations can be carried out in a distributed setting using entanglement. In particular our studies have focused on understanding the (entanglement assisted) communication complexity for arbitrary functions, rather than focussing on specific examples of functions as previous research has done.

Our investigations along these lines have led us into considering a generalization of a problem which as received much attention already, namely the minimal communication requirements (quantum or classical) under which a given entangled state can be transformed into another given state. The generalization we have been investigating, and hope to investigate further, arises when Alice and Bob hold one a set of entangled states (but they don't know which) and they wish to apply some transformation to a different set of entangled states.

To see how this question arises, assume that Alice and Bob initially share a resource of entangled states. They also each have some data, x_A or x_B and wish to compute $f(\, x_A, \, x_B)$. If they each perform some local operations which depend on their input data, we see that they now hold one of a set of possible entangled states - although they do not know which one. Their goal is to perform

operations, with as little classical communication as possible, which result in a different entangled state. This final entangled state we generally envisage being such that one of the parties can tell, from local measurements, what the output $f(x_A, x_B)$ is.

We have begun our investigation into this general question, by looking at the case where Alice and Bob share either the entangled state $|\psi_0\rangle$ or $|\psi_1\rangle$. They wish to effect the transformation

$$\begin{aligned} |\psi_0\rangle &\rightarrow |\phi_0\rangle, \\ |\psi_1\rangle &\rightarrow |\phi_1\rangle, \end{aligned}$$

utilizing as little classical communication as possible. It is well known that if there were only a single state $|\psi\rangle$ which they wished to transform into $|\phi\rangle$, then they can do so with no communication if the two states have the same amount of entanglement. In our only slightly more complex generalization however, no such simple rules are evident. For example, there exists pairs of initial states $|\psi_0\rangle$, $|\psi_1\rangle$ which are orthogonal and have the same amount of entanglement, and corresponding pairs $|\phi_0\rangle$, $|\phi_1\rangle$ of final states which are also orthogonal and which have the same entanglement as the initial states, for which the desired transformation is not (deterministically) possible with no communication.

We have also made the following rather curious observation, which is a special case of the above but for which we are yet to find a concrete application. Imagine that Alice and Bob have an unlimited resource of EPR pairs, and that they use the states $|0_L\rangle = |00\rangle + |11\rangle$ ($|1_L\rangle = |00\rangle - |11\rangle$) to encode a logical zero (one). Note that each of them can set the value of any qubit in the logical basis by a local operation, no communication is required. We have found that on a series of N such encoded logical qubits, Alice and Bob can perform an inversion about average operation (in the logical basis), without *any* communication. They do so by performing a phase inversion on the state with all 0's in the local basis (either party can perform this phase inversion. This result seems to indicate that some form of extended party quantum searching might be possible, we spent considerable time trying to work out the specific communication requirements for this, unfortunately our scheme for quantum searching using entangled states turned out no better than the well known $O\left(\sqrt{N}\right)$ time results for scheduling.

2.11 Quantum searching for classical objects

We believe that some of the earliest uses of results from quantum information processing will be in small but useful applications of quantum effects within a classical computer. The quantum search algorithm was originally phrased in terms of searching an unsorted database for a marked item. Clearly such a database would have to be a "specially constructed quantum" database, and could not be a "regular classical" database. As such the search algorithm is usually thought in terms of querying a (specially constructed) quantum oracle. We have recently shown how to perform a quantum search for a classical object,

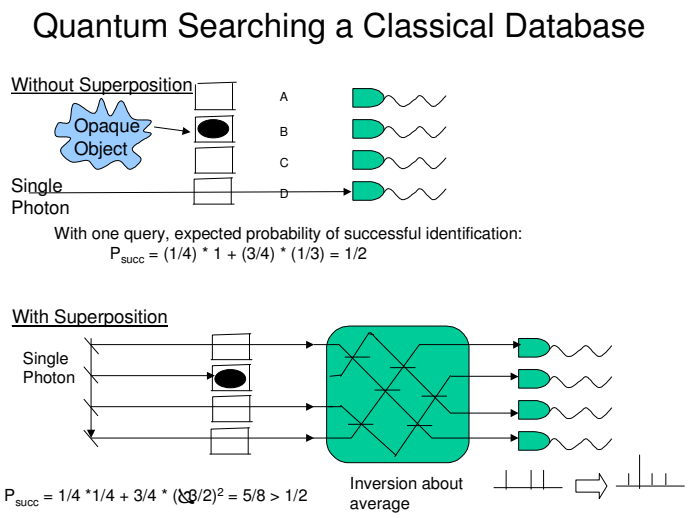

Figure 14: A scheme analogous to quantum search may be used with advantage to search a classical database.

specifically for a classical object which performs no coherent evolution on the quantum computer being used for the search.

The simplest example of such a hybrid quantum/classical process can be understood by considering the case where an opaque object is used to mark one of N different objects, and we are limited to only a single query. Classically the probability of correctly identifying the marked item is $1/N$. However, using appropriate beamsplitters we can place a photon in a superposition of paths corresponding to all N items. In this way the photon queries all items simultaneously. Another array of beamsplitters can then be used to perform an inversion about average operation on the photon paths - it is not difficult to show that our probability of success is now boosted to about $4/N$ in the limit of large N. The following figure gives a detailed calculation of the success probability after a single query to a 4 item database, here too it gives a constant factor improvement over the best possible scheme. As mentioned earlier the loss of the photon due to probing the opaque object limits the success probability.

We have extended this simple one query example, by using interaction free measurement as a subroutine in the quantum search algorithm. This is necessary, because absorptive loss causes the naive one query procedure discussed above to become extremely inefficient after several iterations. Interaction free measurements were invented to answer the question: "Given a bomb which is so sensitive that a single photon touching it will cause it to explode, is there some way to detect the presence or absence of the bomb". It turns out that using quantum mechanics the answer to this unlikely conundrum is "yes". The

mechanism to do so involves the quantum zeno effect, which is used to "mimic" a unitary evolution on the photon with high probability. In our scheme we use this "almost unitary" evolution to act as an oracle type subroutine.

In addition to providing a simple example of how non-unitary processes which approximate unitary ones can be useful in a quantum algorithm, our procedure requires only one photon regardless of the size of the database, thereby giving us a scheme which is provably the most energy efficient scheme to search an arbitrarily large database. Our result can hence be interpreted as showing how to perform an interaction free measurement with a single photon on an arbitrarily large number of possible bomb positions simultaneously. The improvement we have obtained is only by a constant factor - we hope to improve this to a square-root factor (the difference from the standard search algorithm is that there are losses at every step of the classical observation which reduces the amplitudes in all states that give any meaningful information).

It is almost certain that recent developments in searching will lead to some improvements in this algorithm, however, during the course of the last few years, I have not been able to revisit this topic.

3 NP-complete problems

These problems are extremely challenging and researchers in several different fields have been working on them for several decades. We have been working on them intensely - the belief is that even if we are not able to construct a polynomial time algorithm, we hope to find uniquely quantum heuristic algorithms, and we are confident the techniques developed will lead to other spin-offs in our understanding of the strengths and weaknesses of quantum computing. The best known example of such a spin-off is the search algorithm itself as discussed later in this section.

When quantum computing was first being invented, it was hoped that it would be able to solve NP-complete problems just through the *parallelism* of quantum mechanics. Such a scheme would do a brute force search and would not need to use any of the structure of these problems. These hopes were dashed in 1994 by the paper by Bennett, Bernstein, Brassard & Vazirani [BBBV], that proved that the best improvement that such a scheme could provide was a square-root speedup. Indeed, so far the best algorithm for solving NP-complete problems is through a brute force search using the quantum search algorithm which gives a square-root advantage over a classical algorithm; this however, still requires an exponential amount of time. Based on the [BBBV] result, it is often said that quantum computing algorithms could *not* possibly solve NP-complete problems. However, it should be emphasized that this is only true if we look at the NP-complete problem as an exhaustive search problem. NP-complete problems have considerable structure and there well might be other more advantageous ways of looking at them. The science of quantum computation is relatively new and there are several unexplored directions. Farhi and coworkers' recent results on adiabatic evolution were initially suggestive that quantum

algorithms might indeed offer an advantage [Far02]. Even though that has been shown to be unlikely to happen, there are other related directions that appear very promising. We are exploring a number of different algorithms that make use of the power of quantum mechanics to take advantage of the structured nature of these problems.

We plan to investigate how efficiently we can create superpositions that provide information about the solution of computer science problems more effectively than classical probabilistic algorithms. The quantum search algorithm has been shown to be applicable to the synthesis of general superpositions (and hence classical distributions), however it only gives a square-root advantage over classical methods. It remains to be seen what kinds of advantage it gives for structured superpositions. To give an indication of the breadth of possibilities, we mention some approaches we have investigated:

1. One of the issues with NP-complete problems is local optima. As a result, local search algorithms that do a step-by-step improvement, get stuck in local optima and then there is no way of knowing how to proceed. As physicists well know, a feature of quantum mechanical systems is that of tunneling. This might provide systems that can elegantly get out of local optima. Incidentally, when I first designed the quantum search algorithm, I was trying to design a quantum algorithm that had the tunneling ability. Before I could design such a system, I found the search algorithm that derived its speed in a different way.
   Even though we have not yet come up with an local search algorithm for NP-complete problems, this is the approach that appears most promising. Classical local search algorithms are perhaps the most powerful classical algorithms; quantum local search is just starting to get off the ground - e.g. spatial searching. I have my own approach which consists of following the trajectory of a diffusing particle in a confined region. The region can have either reflecting or absorbing boundaries. I have known how to evolve the particle in the presence of absorbing boundaries (provided, of course, the region is convex). Unfortunately this does not conserve the number of particles so one has to design the potential so that there is very high potentials in the region of this absorbing boundary.
   Other ways of getting around this problem are (i) to use binary systems (with the sum of variables as the problem variable) (ii) use Green's theorem to evolve the function (this conserves the integral of the product of the two functions).

2. It is well known how to classically sample according to log-concave distributions. Unfortunately, it is not known how to specify an NP-complete problem as that of sampling a log-concave distribution. We have been able to represent these problems as that of sampling slightly log-convex distributions, i.e. distributions that are slightly non-log-concave at certain well-defined points in certain well defined directions - everywhere else they are log-concave.

It is clear that we can synthesize a quantum mechanical superposition that leads to a log-concave probability distribution by using a variant of the classical algorithm. However, this would be an incoherent distribution and not amenable to further processing on a quantum computer. We have recently discovered a way of synthesizing a quantum superposition corresponding to log-concave distributions that has well defined phases in each state[Gro02c]. Also, we have been able to prove that the magnitudes of the Fourier Transforms of superpositions that correspond to NP-complete problems are log-concave. All that remains is to estimate the phase of an arbitrarily specified point of this superposition. If we can somehow calculate this, we can rotate the phase of each point appropriately and then Fourier Transform back to get the original superposition. Unfortunately, the Fourier Transform of coupled functions is not very amenable to analytical processing such as that we require to prove log-concavity.
After considerable research on this topic, (including Hilbert & Hankel transforms), we are inclined to think that the local search approach is superior. The one opening we see in this direction is to use a min-cut type approach to represent the problem (the advantage is that only the one constraint demanding the sum of the n variables is zero is convex, the rest are all of the same sign). Now when we Fourier transform, all but the one constraint is log-concave and thus amenable to randomized int4egration, it is the one constraint that we have to struggling with.

3. We have been able to represent distributions corresponding to NP-complete problems as products of two simple distributions (in the same variables). Classically, it is not easy to create products of distributions, even though the individual distributions each might be easy to create. Quantum mechanically, one can create the sum of the two superpositions corresponding to the two distributions, then the resulting distribution obtained will have a term corresponding to the product of the two superpositions due to interference effects, i.e. if we think of the superposition: $f_1 + f_2$, then the resulting probability distribution will be: $|f_1|^2 + |f_2|^2 + 2\Re(f_1^* f_2)$. The last term can be designed to give the solution to the NP-complete problem. Unfortunately, this is usually swamped by the first two terms - we spent some time trying to amplify the cross term but this leads to an exponential number of operations. One example is as follows - if we can somehow synthesize the density matrix $|f_1\rangle\langle f_2| + |f_2\rangle\langle f_1|$ (which is symmetric and thus has real eigenvalues), then we can get the desired product state. Unfortunately, the eigenvalues can become negative in general. To ensure positivity of the eigenvalues, one has to add the terms proportional to $|f_1\rangle\langle f_1| + |f_2\rangle\langle f_2|$ - this in essence takes us back to the original pure state situation discussed earlier.

4. In algorithm design, one of the strong points of quantum algorithms is the ease of transforming a superposition into its Fourier Transform, the difficult thing is to convolve together two quantum superpositions. If we can do both the Fourier Transform and convolution, then it is possible to

solve NP-complete problems. Convolving together two classical probabilistic distributions is trivially easy. We have investigated ways of convolving two superpositions, however, after initially promising results, this one did not work out because it required a condition on the log convexity. This is the way the argument goes - assume $f_1(x)$ and $f_2(x)$ are both log-concave in magnitude, then we can clearly create the superposition $f_1(x)f_2(y-x)$, with the x variable as a quantum mechanical variable. The superposition is log-concave for each value of x and hence x can be uncomputed - unfortunately due to the normalization factors, we will be left with the superposition $\frac{\int_x f_1(x)f_2(y-x)\int_x |f_1(x)|^2|f_2(y-x)|^2}{\left|\int_x f_1(x)f_2(y-x)\right|^2}$, which is more complicated than the simple convolution of the superpositions

5. It is possible to solve Schrodinger's Equation, even in non-relativistic quantum mechanics, for certain complicated potentials using supersymmetry . There are well known examples for structures with local optima. We plan to investigate these from an algorithm perspective. For example, superymmetric Hamiltonians often allow an analytic estimate of the eigenvalue gap between the ground state and first excited state. This may allow us to obtain an analytic handle on certain types of adiabatic quantum computation algorithms.[Far02].We even investigated systems with a single bound state, since this is guaranteed to be separated from the unbound state by a finite amount, the gap can be easily controlled, however we could not attain comparable results for multi-dimensional systems.

   The most promising approach we tried was to examine a system with a single bound state (in multiple dimensions, even fairly wide potentials have only a few bound states) - for example consider a potential function that is the product of n one dimensional wells, each with a single bound state. Now if we consider perturbing this product by a quadratic potential function of the form $\sum_{i,j} c_{ij}x_ix_j$, we can arrange for this ground state to be concentrated in the region of the minimum potential function. Unfortunately introducing a quadratic potential function means introducing multiple bound states too.

6. At the moment the approach that looks promising is the followingt - implementing R_0 by interaction with unperturbed states. The idea is to have many instances of the superposition and in each instance randomly choose the coordinate to be operated on. Then since the average of all superpositions is very close to the 0 state, this is the one to be inverted (inverting the average is easy as everyone familiar with the search algorithm knows!)

Progress in Topological Quantum Computing

The task of building a scalable quantum computer remains one of the most compelling and challenging problems of our time. While many approaches have been proposed for reaching this goal, and while much has been achieved experimentally, there still remains an enormous gap between our current status and

the final goal. It appears that nature has not been very generous in allowing us to suppress decoherence in any easy way.

Recently, one particular approach has arisen that proposes to beat the decoherence problem in a very different way than all other schemes. This approach, known as *topological quantum computation* relies on exotic states of matter that in essence have quantum error protection built into their ground states (For a very thorough introduction and review of this idea, see [1]). While experimentally this approach lags behind other schemes, having not even achieved a single qubit, the long term promise of built-in protection from decoherence is appealing enough to have attracted substantial interest.

Over the past few years the group at Bell Labs has been very focused on making progress on topological quantum computing both experimentally and theoretically. Experimentally, the drive to achieve topological quantum computation is beginning with a more detailed study of certain fractional quantum Hall states Ð the only known states of matter that are believed to be capable of topological computation. Bell Labs has led the world in the study of fractional quantum Hall physics for over two decades, and still dominates the field. Much of this dominance is due to our*unique* ability to grow ultra-pure Gallium-Arsenide semiconductors that are required for producing the fractional quantum Hall states. Indeed, every experimental group in the world that collaborates with Bell.

On the theoretical front, Dr. Simon has been studying topological algorithms. In topological quantum computation, a universal quantum computation is performed by moving particles around each other in complex patterns to form space-time braids (See [1]). The interesting algorithmic problem is then to figure out what patterns (or what braids) perform which computations [2-3]

[1]NonAbelian Anyons and Topological Quantum Computation, C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. DasSarma, to be published in Rev. Mod. Phys; arXiv:0707.1889

[2] Braid Topologies for Quantum Computation, N. E. Bonesteel, L. Hormozi, G. Zikos, and S. H. Simon, Phys. Rev. Lett. 95, 140503, (2005).

[3] Topological Quantum Computing with Only One Mobile Quasiparticle, S. H. Simon, N. E. Bonesteel, M. H. Freedman, N. Petrovic, and L. Hormozi, Phys. Rev. Lett. 96, 070503 (2006).

[4] Topological quantum compiling, L. Hormozi, G. Zikos, N. E. Bonesteel, and S. H. Simon, Phys. Rev. B 75, 165310 (2007).

4 Conclusion

Quantum search was a surprising result because it gave an $O(\sqrt(N))$ step algorithm to find a single marked item in an unsorted database of size N. It took some time for the scientific community to absorb this result. There are N items, so one would expect that it should need N steps to search them since . However, this is only true if one thinks classically, quantum systems are not subject to these limitations, they can be in multiple states and examine multiple items at

the same time. There is thus no clear limit as to how fast these can search the database.

The second surprising fact about this algorithm was that soon after it was discovered it was proved to be optimal. This was surprising because I had made no particular attempts to optimize it. As a consequence of this optimality proof, most of the research that has been done on this is to increase the scope of its applicability through amplitude amplification.

The third surprising result was that even after more than twelve years of intense research (it is one of the most researched topics in the field of quantum computing), it continues to yield fundamentally new results). This report describes some of these results.

5 Personnel

1. ***Lov K. Grover***:

   He was the main researcher in this program. As mentioned in the text of this proposal, he has pioneered some of the ground-breaking recent concepts in quantum computation. In recognition of his achievements, Bell Labs promoted him to a Distinguished Member of Technical Staff. He has been at Bell Labs, Murray Hill since 1994. Prior to that he was a faculty member in the School of Electrical Engineering at Cornell University. He got his Ph.D. in Electrical Engineering and an M.S. in Physics from Stanford University in 1984 and an M.S. in Electrical Engineering from Caltech in 1982. He got his B. Tech. in Electrical Engineering from IIT (Indian Institute of Technology, New Delhi, India) in 1981.

2. ***Terry Rudolph:***

   Dr. Rudolph is a post-doctoral fellow at Bell Labs. He is a theoretician most recently from the Institute for Experimental Physics at the University of Vienna. Prior to that he was a faculty member at the University of Toronto. Dr. Rudolph completed his PhD in 1998 (at age 24), in the field of theoretical quantum optics. He still collaborates intensively with members of the experimental quantum optics community on problems associated to practical implementations of quantum computing. Within the field of quantum information, Dr. Rudolph has authored over ten papers, and is particularly known for his fundamental work on two-party quantum cryptographic protocols. In his keynote address at the Workshop on Quantum Computing in Huangshan, China in September 2001, Charlie Bennett prominently referred to him as *the world's leading expert on direction finding*. He has recently accepted a faculty position at Imperial College, London, UK.

3. *Steven H. Simon*

   He is the director of Quantum Information and Semiconductor Physics at Alcatel-Lucent Bell Labs. He is a theoretician with broad expertise

in condensed matter physics, quantum Hall physics, information theory, communications theory, and quantum computation. His recent research has focused on topological quantum computation. He has been at Bell Labs since 1997 and was elevated to department director in 2000. Since then he has managed research efforts in a broad range of fields ranging from biological computation to complex systems to quantum information. Prior to being at Bell Labs he was a postdoctoral researcher at MIT. He obtained a Ph.D. at Harvard in 1995 and a B.Sc. at Brown Univerisity in 1989. He holds five patents and is a fellow of the American Physical Society.

4. *Tathagat Tulsi*

   Tathagat Avatar Tulsi is is most well known as a child prodigy and holder of Guinness World Records. He completed high school at the age of nine, earned a B.Sc. at the age of ten and a M.Sc. at the age of twelve.

   He is just completing his Ph.D. at Indian Institute of Science, Bangalore, India in the field of quantum computing in which he has done some truly outstanding work. He is mostly known as a child prodigy, unfortunately his technical work which is of an equally high caliber is nowhere as well known as it deserves to be. His invention of the fixed-point quantum search algorithm after listening to my talk at a workshop in IIT Kharagpur, is one of the most intriguing, though not widely known stories, in the field.

   I had discovered the $\pi/3$ phase shift algorithm after almost 10 years of fiddling around with the original search algorithm, countless other scientists in the field too had closely studied the algorithm (it is one of the most well studied results in the field), yet no one had noticed that by having a $\pi/3$ phase shift instead of a π phase shift, the algorithm assumed a radically new form - the original search algorithm was based on delicate interference effects and was very sensitive to problem parameters, e.g. if the number of solutions is not known, the performance of the algorithm suffers greatly. Quite surprisingly, this sensitivity property is greatly improved by having a $\pi/3$ phase shift instead of a π phase shift. I gave a routine talk about this new algorithm in a workshop at IIT Kharagpur which Tathagat happened to be attending. A few days later he had invented his own variant of the search algorithm which was every bit as good as the one I had (the one I had discovered had been proved to be optimal).

   After this amazing discovery, he spent about 6 months at Bell Labs supported by the ARO contract.

   Norm Margolus & *Jaikumar Radhakrishnan* were two other prominent researchers supported under this contract.

6 Papers that appeared during this period

1. Quantum State Targeting Terry Rudolph and Rob Spekkens. quant-ph/0310060 Phys. Rev. A. 70, 052306 (2004).

2. How significant are the known collision and element distinctness quantum algorithms? Lov Grover and Terry Rudolph quant-ph/0309123 Journal Quantum Information & Computation ,4, 201 (2004).

3. Photon number superselection and the entangled coherent state representation Barry C. Sanders, Stephen D. Bartlett, Terry Rudolph, Peter L. Knight quant-ph/0306076 Phys. Rev. A. 68, 042329 (2003).

4. On the communication complexity of establishing a shared reference frame Terry Rudolph and Lov Grover quant-ph/0306017 Phys. Rev. Lett. 91, 217905 (2003). (The key idea in our paper on communication complexity of a shared reference frame was turned into an optical phase estimation style problem the experiment of which was published in Nature: http://arxiv.org/abs/0709.2996)

5. On continuous-variable entanglement with and without phase references, S.J. van Enk, Terry Rudolph quant-ph/0303096

6. Unambiguous discrimination of mixed states, Terry Rudolph, Robert W. Spekkens and Peter Shipley Turner quant-ph/0303071 Phys. Rev. A. 68, R010301 (2003).

7. Classical and quantum communication without a shared reference frame, Stephen D. Bartlett, Terry Rudolph, R. W. Spekkens, quant-ph/0302111 Phys. Rev. Lett. 89, 227901 (2001).

8. Quantum communication protocols using the vacuum, Xiatra Anderson, S.J. van Enk, Terry Rudolph, quant-ph/0302091 Journal Quantum Information & Computation, 3, 423 (2003).

9. A 2 rebit gate universal for quantum computing Terry Rudolph and Lov Grover quant-ph/0210187

10. Creating superpositions that correspond to efficiently integrable probability distributions Lov Grover and Terry Rudolph, quant-ph/0208112

11. Constructing physically intuitive graph invariants Terry Rudolph, quant-ph/0206068

12. Evolution in time of an N-atom system. II. Calculation of the eigenstates Terry Rudolph, Itay Yavin and Helen Freedhoff, quant-ph/0206067 Phys. Rev. A. 69, 013815 (2004).

13. Quantum searching a classical database (or how we learned to stop worrying and love the bomb) Terry Rudolph and Dr.(Strange)Lov Grover, quant-ph/0206066

14. The laws of physics and cryptographic security Terry Rudolph, quant-ph/0202143

15. A quantum protocol for cheat-sensitive weak coin flipping Rob Spekkens and Terry Rudolph, quant-ph/0202118 Phys. Rev. Lett. 89, 227901 (2001).

16. Comment on "The Quantum State of a Propagating Laser Field Terry Rudolph and Barry C. Sanders quant-ph/0112020

17. A simple gate for linear optics quantum computing, T. Rudolph and J.-W. Pan, quant-ph/0108056

18. Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol, Rob Spekkens and Terry Rudolph, quant-ph/0107042 Journal Quantum Information

19. Avatar Tulsi, "Adiabatic Quantum Computation starting with a 1-D projector Hamiltonian", Accepted for publication in Phys. Rev. A. quant-ph/0806.0385.

20. Avatar Tulsi, "Faster quantum-walk algorithm for the two-dimensional spatial search" , To appear in Phys. Rev. A. quant-ph/0801.0497

21. Avatar Tulsi, "Quantum computers can search rapidly by using almost any selective transformation" To appear in Phys. Rev. A. quant-ph/0711.4299

22. Fixed-point quantum searching, Lov K. Grover, Physical Review Letters, Vol. 95, Pages 150501, October 7, 2005.

23. Quantum Error Correction of Systematic Errors using a Quantum Search Framework, Ben Reichardt & Lov K. Grover, Physical Review A 72, 042326, October 25, 2005.

24. Preserving Quantum States - A super-Zeno effect, Deepak Dhar, Lov K. Grover, Shasanka Roy, Physical Review Letters, Volume 96, issue 10, March 16, 2006.

25. A new algorithm for directed quantum search, T. Tulsi, L. Grover, and A. Patel, Quantum Information & Computation, Volume 6, No. 6, September 2006.

26. Simple Algorithm for partial quantum search, Vladimir Korepin & Lov K. Grover, Quantum Information Processing, vol. 5, number 1, page 5-10, 2006.

27. Is partial quantum searching of a database any easier? Proceedings SPAA, 2005, Jaikumar Radhakrishnan and Lov K. Grover.

28. Superlinear amplitude amplification, Lov Grover, quant-ph - June 3, 2008.

References

[Gro96] L. K. Grover, "Quantum Mechanics helps in searching for a needle in a haystack", *Phys. Rev. Letters*, 78(2), 325, 1997, also at http://www.bell-labs.com/user/lkgrover/.

[Gro01] L. K. Grover, "From Schrodinger's Equation to the Quantum Search Algorithm", American Journal of Physics, May 2001, also at http://www.bell-labs.com/user/lkgrover/.

[Zal99] C. Zalka, "Grover's quantum searching is optimal," Phys. Rev. A 60, 2746 (1999).

[Bra98] Michel Boyer, Gilles Brassard, Peter Hoeyer, Alain Tapp, "Tight bounds on quantum searching," Fortsch. Phys. 46 (1998) 493-506.

[Got99] D. Gottesman and I. Chuang, Nature **402,** 390 (1999).

[Rau01] R. Raussendorf and H. Briegel, Phys. Rev. Lett., 5188 (2001).

[Nie01] M. Nielsen, quant-ph/0108020.

[Ort01] G. Ortiz et al., Phys. Rev. A. 64, 022319 (2001); R. Somma et. al., quant-ph/0108146.

[Kit00] M. Freedman, A. Kitaev and Z. Wang, quant-ph/0001071.

[Fre01] M. Freedman et. al. quant-ph/0101025.

[Adl97] L. Adleman, J. Demarrais and M-D. A. Huang, Siam.J. Comput. **26**, 1524 (1997).

[Ben97] C. H. Bennett, E. Bernstein, G. Brassard & U.Vazirani, SIAM Journal on Computing, 26, no. 5, Oct. 1997, p. 1510-1524.

[Far02] E. Farhi, et al., quant-ph/0201031.

[Far98] E. Farhi and S. Gutmann, Phys. Rev. A 58, 915-928 (1998)

[Coo01] F. Cooper, A.Khare and U. Sukhatme, *Supersymmetry in Quantum Mechanics*, World Scientific (2001).

[Kwi95] P. Kwiat et. al., Phys. Rev. Lett. **74**, 4763 (1995).

[Gro02a] L. K. Grover, "An Improved Quantum Scheduling Algorithm", quant-ph/0202033.

[Gro02b] L. K. Grover, "Tradeoffs in the Quantum Search Algorithm", quant-ph/0201152.

[Gro02c] L. K. Grover and T. Rudolph, "Creating superpositions that correspond to efficiently integrable probability distributions", quant-ph/0208112.

[Kas02] E. Kashefi et al, Phys. Rev. A 65 050304 (2002).